



ENJOY SAFER TECHNOLOGY™

Le 10 Mars 2015

COMMUNIQUE DE PRESSE

La Syrie ciblée par le logiciel malveillant CASPER

Les chercheurs ESET analysent Casper, le dernier malware espion du groupe cybercriminel derrière Babar et Bunny également.

Le groupe d'espions a encore frappé ! Après [Bunny](#) et [Babar the Elephant](#), les cybercriminels ont développé un autre malware du type, nommé Casper. Cet outil de reconnaissance est en mesure d'envoyer un rapport détaillé de la machine de la victime lorsqu'elle est touchée par l'attaque de Casper, au cybercriminel qui la contrôle.



C'est en avril 2014, lors de l'attaque de quelques victimes en Syrie, qu'a été détecté Casper pour la première fois. Les hackers ont utilisé l'Exploit zéro-day pour infiltrer la faille CVE-2014-0515, niché dans le plugin Adobe [Flash](#). Ce qui les a aidés à connaître les détails de la machine infectée et de pouvoir décider des prochaines étapes, le tout sans se faire remarquer.

« Un fait intéressant est que ces exploits ont été hébergés sur un site appartenant au Ministère de la Justice syrienne : [jplic.gov.sy](#), site internet créé par le gouvernement syrien qui sert aux habitants à envoyer leurs plaintes. Il existe toujours mais a été nettoyé. Par ailleurs, le logiciel espion Casper était aussi hébergé sur ce même site pour y déployer des plugins qui s'étaient exécutés sur la machine. » explique le chercheur en logiciels malveillants d'ESET, Joan Calvet.

Basés sur les observations et analyses des logiciels malveillants, les chercheurs ESET confirment que le code correspond à ceux utilisés par Babar et Bunny. Mais Casper a franchi une étape supplémentaire en adaptant sa stratégie en fonction du logiciel de sécurité installé sur les machines ciblées. C'est pour cela que pratiquement aucun antivirus ou logiciel de sécurité online n'a été capable de le détecter, excepté [ESET LiveGrid®](#). Malgré son aspect très sophistiqué, le malware n'a attaqué que très peu de gens à ce jour, tous localisés en Syrie.

Pour en savoir plus, lisez [le rapport de Joan Calvet sur WeLiveSecurity.com](#).

À propos d'ESET

Fondée en 1992, la société ESET est spécialisée dans la conception et le développement de logiciels de sécurité pour les entreprises et le grand public. Pionnier en matière de détection proactive des menaces véhiculées par l'Internet, ESET est aujourd'hui le leader dans ce domaine. À ce jour, l'antivirus ESET Nod32 détient le record mondial de récompenses décernées par le laboratoire indépendant Virus Bulletin depuis 1998. ESET Nod32, ESET Smart Security et ESET Cybersecurity pour Mac sont reconnus et appréciés par des millions d'utilisateurs dans le monde.

À propos d'Africa Global Services

Créée en 2011, Africa Global Services est spécialisée dans la sécurité IT principalement destinée aux professionnels. Son panel de solutions couvre aujourd'hui tous les aspects de la sécurité et apporte des réponses aux différents problèmes que rencontrent quotidiennement les DSI. Qu'il s'agisse de solutions antivirus, plan de reprise d'activité après sinistre, filtrage ou encore problématiques liées à l'authentification forte et BYOD, Africa Global Services a les solutions adéquates.

Africa Global Services représente aujourd'hui une dizaine de marques de premier plan dont ESET (NOD32 Antivirus), StorageCraft, Double-Take, 8MAN, SMS Passcode. Les solutions sont rigoureusement sélectionnées et choisies, tant pour leurs performances, leurs qualités et fiabilité, que pour la pérennité de l'éditeur. Elle offre aux entreprises de toutes tailles, des solutions innovantes couvrant tous les aspects de la sécurité nécessaires aux entreprises. De la TPE aux grandes entreprises, Africa Global Services a des solutions adaptées à tous les fondamentaux de la protection des données.

Représentants des éditeurs distribués au Maghreb et en Afrique Francophone de manière exclusive et par conséquent proposition de tous les services intégrés et localisés pour les entreprises : support, déploiement, transfert de compétences, formation, certification et conseils font parties de sa valeur ajoutée.

Africa Global Services travaille avec les entreprises de manière indirecte par l'intermédiaire de ses revendeurs agréés dans chacun de ses 22 pays.

Pour en savoir plus, veuillez visiter le site Internet : www.africa-gs.com

CONTACT PRESSE

Marketing-Land

Marion Lecrique | RP

e-mail | marion.l@marketing-land.com

mobile | 06 81 78 23 34

Fixe |

